



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/978,200

10/17/2001

Paul Neil Fahn

06944.0049

4160

27871

7590

01/12/2006

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER

KHOSHNOODI, NADIA

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 01/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/978,200	FAHN ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/26/2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 October 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to amended claims 1-3, 7, 10, 13, & 17-18 and previously presented claims 4-6, 8-9, 11-12, & 14-16 filed 10/26/2005 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Examiner would like to note that all previous objections to the specification/drawings are withdrawn due to the amendments filed 10/26/2005. Furthermore, the previous 35 U.S.C. 112, second paragraph and 35 U.S.C. 101 rejections are also withdrawn.

Response to Arguments

Applicant contends that Asay et al. do not teach or suggest generation of a string from information in the certificate request. Examiner respectfully disagrees. Asay et al. teach that when a user requests an original certificate from a certain certification authority, the unique identifier is generated based on a combination of the issuer's identity and a serial number that identifies the certificate, i.e. the string is generated from information in the certificate request (col. 11, lines 15-31). Furthermore, Asay et al. also teach that the certificate is stored in a readily retrievable manner, meaning that once the certificate to be retrieved is identified by the unique identifier the certificate is located (col. 14, lines 25-42). In other instances, Asay et al. discuss the basics of how certificates are issued. Asay et al. teach that when the certificate authority issues a certificate, one of the rules is that the certificate authority must ensure that the certificate being issued is properly issued to the correct person, i.e. the public key for the certificate must be

Art Unit: 2137

derived from the private key of the person requesting the certificate. Therefore, even the public key is generated based off of the individual requesting the certificate to uniquely identify the certificate so that it may ultimately be located and retrieved when necessary (col. 1, lines 53-65).

Applicant also contends that Asay et al. do not teach or suggest utilizing a string to obtain the address of a certificate. Examiner respectfully disagrees. Asay et al. teach that the certificates are stored in a readily accessible manner. Asay et al. also teach that once identified, where the unique identifier was previously generated to uniquely distinguish one certificate from another, the certificate may be accessed (col. 14, lines 25-42). Furthermore, Asay et al. suggest that the primary certificate may contain either an address where that certificate is located or alternatively that a pointer to an address, i.e. a string that points to the location of the certificate, may be used (col. 18, lines 20-45).

Due to the reasons stated above, the Examiner maintains rejections with respect to amended claims 1-3, 7, 10, 13, & 17-18 and previously presented claims 4-6, 8-9, 11-12, & 14-16. Asay et al. teach and suggest motivation for modifying the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that amended claims 1-3, 7, 10, 13, & 17-18 and previously presented claims 4-6, 8-9, 11-12, & 14-16 are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2137

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

IV. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al., U.S. Patent No. 5,903,882.

As per claim 1:

Asay et al. substantially teach a method of allocating an address to a certificate to be stored in an addressable database for subsequent retrieval, said method comprising the steps of generating a string for use as a certificate locator from information contained in a certificate request (col. 18, lines 12-20). Not explicitly disclosed is utilizing said string to obtain said address. However, Asay et al. teach that the identifier is used in order to gain access to the primary certificate, where the primary certificate then contains information regarding the reliance server's address containing validity information for the primary certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to directly obtain the address of the certificate in the reliance server by using the generated string. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 21-32.

As per claim 2:

Asay et al. substantially teach the method according to claim 1. Not explicitly disclosed is the method wherein said string is mapped to an address in a directory. However, Asay et al. teach that the identifier for the primary certificate is the string used in order to gain access to the information of the primary certificate which includes an address for the reliance server which

Art Unit: 2137

contains further identification information for the primary certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to directly map the identifier used to obtain the primary certificate to the address of the reliance server. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 19-28.

As per claim 3:

Asay et al. substantially teach the method according to claim 1. Furthermore, Asay et al. teach wherein said string is used as said address in said directory (col. 18, lines 19-25).

As per claim 4:

Asay et al. substantially teach the method according to claim 1. Not explicitly disclosed is the method wherein a mathematical function is applied to said information to obtain said string. However, Asay et al. teach that the identifier of the primary certificate contains the subscriber's public key, which is derived from some type of mathematical function that has been applied to information. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to have a predetermined mathematical function applied to the information in order to obtain the string. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 19-20.

As per claim 5:

Asay et al. substantially teach the method according to claim 4. Not explicitly disclosed is wherein said mathematical function is a hash function. However, Asay et al. teach that the subscriber's public key can also be used as the identifier for a certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to compute the string by applying a cryptographic hash function to at least part of the request. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 1, lines 45-52 and col. 36, lines 22-29.

As per claim 6:

Asay et al. substantially teach the method according to claim 5. Not explicitly disclosed is wherein said string is a portion of the output of said hash function. However, Asay et al. teach that the subscriber's public key can also be used as the identifier for a certificate. Furthermore, the value of the public key can be a portion of what the hash function outputs, depending on the algorithm. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to compute the string by applying a cryptographic hash function to at least part of the request. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 1, lines 45-52 and col. 36, lines 22-29.

As per claim 7:

Asay et al. substantially teach the method of identifying an address of a certificate to a recipient of a signed message in a data communication system, said method comprising the steps

of preparing a set of information for inclusion in a certificate request (col. 18, lines 16-55), generating from said set of information a string for use as a certificate locator in a database (col. 18, lines 19-20). Not explicitly disclosed is forwarding said string to said recipient to indicate the location of said certificate in said database. However, Asay et al. teach that the identifier for the primary certificate is the string used in order to gain access to the information of the primary certificate which then allows information regarding the address for the reliance server which contains further identification information for the primary certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to forward the reliance server database's address to the recipient to indicate the location of the certificate in that database allowing access to further identification information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 19-45.

As per claim 8:

Asay et al. teach the method according to claim 7. Not explicitly disclosed by Asay et al. is wherein said information includes a time varying element. However, Asay et al. teach that the primary certificate has a field which verifies whether or not the certificate is valid based on time constraints. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to include the time-varying element in the information that is ultimately used in order to generate the string identifier. This modification would have been obvious because a person having ordinary skill in the art, at the time the

Art Unit: 2137

invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 5, lines 44-51 and fig. 1, element "validity period."

As per claim 9:

Asay et al. substantially teach the method according to claim 7. Not explicitly disclosed is the method wherein a predetermined mathematical function is applied to said information to obtain said string. However, Asay et al. teach that the identifier of the primary certificate contains the subscriber's public key, which is derived from some type of mathematical function that has been applied to information. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to have a predetermined mathematical function applied to the information in order to obtain the string. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 19-20.

As per claim 10:

Asay et al. substantially teach a method for maintaining certificates in a public key infrastructure having a certification authority and a pair of correspondents, said method comprising the steps of collating at one of said correspondents information comprising storing the certificate authority's certificate information in the certificate (col. 11, lines 15-42), computing from said information comprising said request a string for use as a certificate locator by said one correspondent and said certification authority (col. 12, lines 16-39 and col. 14, lines 16-34), storing a certificate issued from said request in a directory at an address obtained from

said string and forwarding said locator from said one correspondent to another permit retrieval of said certificate from said directory (col. 14, lines 27-42).

Not explicitly disclosed is the method comprising a request for a certificate of said certification authority, forwarding said request to said certification authority. However, Asay et al. teach that the certificate authority's certificate information can be included in the primary certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to request that information from the certificate authority thereby forwarding the request for that certificate information to the CA. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 5, lines 2-11.

As per claim 11:

Asay et al. teach the method according to claim 10. Not explicitly disclosed by Asay et al. is wherein said information includes a time varying element. However, Asay et al. teach that the primary certificate has a field which verifies whether or not the certificate is valid based on time constraints. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to include the time-varying element in the information that is ultimately used in order to generate the string identifier. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 5, lines 44-51 and fig. 1, element "validity period."

As per claim 12:

Asay et al. substantially teach the method according to claim 10. Not explicitly disclosed is wherein communication between said one correspondent and said certification authority is performed over a secure channel. However, Asay et al. teach the use of encrypting certain data in the certificate in order for that data to remain confidential when being transmitted.

Furthermore, it is well known that the secure channel is used in order to encrypt data when being transmitted for that same purpose. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. for the communication to occur over a secure channel so that no information, especially sensitive information that can be found in the certificates, is compromised. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 11, lines 38-42.

As per claim 13:

Asay et al. substantially teach the method according to claim 10. Not explicitly disclosed is wherein said other correspondent obtains an address of said certificate from a known address of said directory and said string. However, Asay et al teach that in order to gain access to the primary certificate, a certificate identifier must be used. Furthermore, Asay et al. teach that once that primary certificate is found, it contains an address to the reliance server which is used for the secondary certificates. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to obtain an address of the second certificate by using the string to access the location of the primary certificate in the directory. This modification would have been obvious because a person having ordinary skill in

Art Unit: 2137

the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 16-45.

As per claim 14:

Asay et al. substantially teach the method according to claim 10. Not explicitly disclosed is the method wherein said other correspondent forwards said locator to said certification authority for construction of said address. However, Asay et al. teach that there can be different reliance servers that maintain further identification information in order to allow issuance of a second certificate based on the primary certificate issued, where the location of the reliance server must be apparent in the primary certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. for the correspondent to forward the locator to the certificate authority in order to construct the address. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 25-45.

As per claim 15:

Asay et al. substantially teach the method according to claim 10. Not explicitly disclosed is wherein said string is computed by application of a cryptographic hash function at least part of said request. However, Asay et al. teach that the subscriber's public key can also be used as the identifier for a certificate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to compute the string by applying a cryptographic hash function to at least part of the request. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was

made, would have been motivated to do so since it is suggested by Asay et al. in col. 36, lines 22-29.

As per claim 16:

Asay et al. teach the method according to claim 15. Not explicitly disclosed by Asay et al. is wherein said information includes a time varying element. However, Asay et al. teach that the primary certificate has a field which verifies whether or not the certificate is valid based on time constraints. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to include the time-varying element in the information that is ultimately used in order to generate the string identifier. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 5, lines 44-51 and fig. 1, element "validity period."

As per claim 17:

Asay et al. substantially teach the method according to claim 15. Not explicitly disclosed is wherein said string is a portion of the output of said hash function is used as the string. However, Asay et al. teach that the subscriber's public key can also be used as the identifier for a certificate. Furthermore, the value of the public key can be a portion of what the hash function outputs, depending on the algorithm. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. to compute the string by applying a cryptographic hash function to at least part of the request. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in

col. 1, lines 45-52 and col. 36, lines 22-29.

As per claim 18:

Asay et al. substantially teach the method according to claim 10. Not explicitly disclosed is wherein said bit string is utilized as a pointer to an address in a directory. However, Asay et al. teach that the primary certificate can hold a pointer to the address of the reliance server where the second certificate is maintained. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asay et al. for the string to be utilized as a pointer to an address in a directory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Asay et al. in col. 18, lines 25-28.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 5,922,074
2. US Patent No. 6,823,454
3. US Patent No. 6,795,920
4. US Pub. No. 2001/0016851
5. US Pub. No. 2004/0054890

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.


Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Nadia Khoshnoodi
Examiner
Art Unit 2137
1/5/2006

NK


MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137